ABSTRACT

The invention relates to password-based authentication in group networks. Each device has an authentication token irreversibly based on the password. The authentication involves a first device at which the password P is entered and a second device towards which the authentication occurs. The first device determines a check token M_j for the second based on the password and its own authentication token R_I and this check token is sent to the second device, where it is compared with the authentication token of that device. The procedure may include update of a device to exclude a non-trusted device from the group or change the password. Advantageous features are that the information in one device does not allow retrieval of the password and that the password is only exposed at one device, and only temporarily, during the authentication.